International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 1– No.8, April 2012 – www.ijais.org

Cogent Sharing Of Covert File Using Audio Cryptographic Scheme

P. V. Khobragade
Department of Computer Engineering,
Sinhgad Academy of Engineering,
Pune, Maharashtra

Nilesh Uke
Department of Information Technology,
Sinhgad College of Engineering,
Pune, Maharashtra

ABSTRACT

In an audio secret sharing scheme, the shares are created by embedding the secret message into an audio file. The audio or the music file which is used to embed the given message is called cover sound. A 2-out-of-2 audio cryptography is a secret sharing scheme that can be used to hide a digital message into 2 shares and we can perceive the message by playing these 2 sounds simultaneously. In this paper a new (2, 2) audio cryptography scheme is proposed. The proposed scheme hides a digital secret message into two audio files. The original secret sound or audio file can be recovered back by playing simultaneously both the audio files.

Keywords

Audio Cryptography, Secret Sharing, Cover Sound, Visual Cryptography, Threshold Scheme

1. INTRODUCTION

Secret sharing is a method to distribute a secret between some participants such that particular subsets could retrieve the secret when their shares come together [1]. Secret sharing was first introduced by Blakley [2] and Shamir [3] in 1979, independently. In 1994, Naor and Shamir proposed a new (*k*, *n*) threshold visual secret sharing scheme [4], in which visual secret is reconstructed back without any computation.

Audio Secret Sharing Scheme (ASSS) is a special type of secret sharing scheme in which the shares are created by embedding the secret data into the cover sound where cover sound represent the sound used to hide the data. On the other hand, an audio file can be a secret file of which shares can be created. In 1998, Desmedt, Hou, and Quisquater (DHQ) [5] first proposed the (2, 2) audio secret sharing (ASS) scheme. The main goal of the DHQ ASS scheme is to embed a binary secret message by cover sound, such as harmonic sound or high quality music. For example, in the DHQ (2, 2) ASS scheme, the human “ears” can decode the concealed message if one plays two shares simultaneously. Desmedt et al. also proposed the generalized DHQ (2, *n*) ASS scheme based on their (2, 2) ASS scheme using [log2n] different cover sounds.

Lin et al. in 2003 proposed a new audio secret sharing scheme which uses the technique of time division with only one cover sound. [7] The effect of this is that when enough shares are played simultaneously the human auditory system can detect changes in the sound volume. Destructive interference results in low volume, while constructive interference results in high volume. The changes in the sound volume reveal the secret binary message, in the sense that the high volume segment corresponds to 1 and the low volume segment corresponds to 0.

Daniel Socek in 2005 proposed a new type of cryptographic scheme which is analogous with visual cryptography. This scheme is based on a different principle. Instead of using sound interference, focus is on using two types of flat frequencies (beeps): the short beep and the long beep. This kind of sound is similar to a Morse code signal [8]. Dealer represents *m*-bit secret binary message as a short-beep long-beep audio signal *S* .For every bit, dealer tosses a coin depending on the outcome, the beep is shared in two shares.

Mohammad Ehdaie et al. have done similar work. They had implemented (k, n) audio cryptography scheme in that n shares are created for encryption and k shares are used for decryption. Audio share files are thus created and audio secret is obtained only by playing *k* shares, simultaneously, each of this is amplified by a certain coefficient. Therefore, the secret is reconstructed without any computation. They had implemented this scheme using MATLAB [9].Actually in this scheme they had divided audio file into small intervals referring to the ith interval as $A_{i.}$ and finding the vector array. Then finally multiplying the every value of $A_{i.,}$ with some constant value c.

The threshold scheme is helpful in the management of cryptographic keys. The most secure key management scheme keeps the key in a single, well secured place but this scheme is highly unreliable since a single misfortune can make the information inaccessible. By using a *(k, n)* threshold scheme with n=2k-1 we get a very robust key management scheme we can recover the original key even when [n/2] =k-1 of the remaining k pieces. [3].If sufficient numbers of shares are come together we will get the original key or password.

In this paper a new (2, 2) Audio Cryptography Scheme for the wave file is proposed which is very simple and efficient.

2. PREVIOUS WORK

Desmedt et al first proposed the (2, 2) audio secret sharing (ASS) scheme. This scheme can be explained as follows: suppose S denotes the plaintext message, L denotes the length of the embedded message; T denotes the length of secret bit (seconds). Then to encrypt the plaintext message *S*, by deciding the high (bit 1) or low (bit 0) volume, There is a random selection of a phase .It may be either 0 or π. Therefore in the first share, select the phase as 0 or π and by selecting the exactly opposite phase in the second share as shown in Figure 1. Each share will have phases “0” and “π”, half and half, in every time slot *Tb*, and fixed amplitude A. so volume change for each share is not recognized.

When adding both the shares particularly by playing different sounds from two speakers, we will get the amplitude 2A in time slot where the plaintext message is 1. Finally, we are able to hear the volume change and recover the secret *S*.

Figure 2. shows the 2-out-of-2 audio cryptography scheme illustration.

Volume	H		L	
Share S1	0	π	0	Π
Share S2	0	π	π	0

Figure 1: The choice of phase for each share

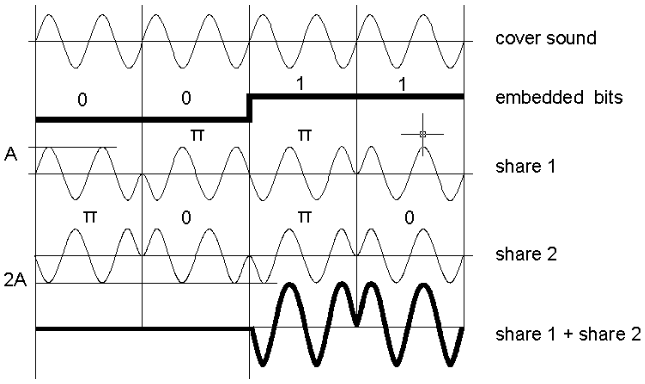


Figure 2: 2-out-of-2 audio cryptography scheme

3. PROPOSED SCHEME

The proposed scheme is based on audio distribution among different channel. So before proceeding further we first look wave file format [10].

The WAVE file format is a subset of Microsoft's RIFF specification for the storage of multimedia files. A RIFF file starts out with a file header followed by a sequence of data chunks. A WAVE file is often just a RIFF file with a single "WAVE" chunk which consists of two sub-chunks -- a "fmt" chunk specifying the data format and a "data" chunk containing the actual sample data. Call this form the "Canonical form". As an example, here are the opening 72 bytes of a WAVE file with bytes shown as hexadecimal numbers:

52 49 46 46 24 08 00 00 57 41 56 45 66 6d 74 20 10 00 00 00 01 00 02 00

22 56 00 00 88 58 01 00 04 00 10 00 64 61 74 61 00 08 00 00 00 00 00 00

24 17 1e f3 3c 13 3c 14 16 f9 18 f9 34 e7 23 a6 3c f2 24 f2 11 ce 1a 0d

Now we will see the meaning of each byte as a WAVE sound file:

A	B	C	D
a	b	c	d

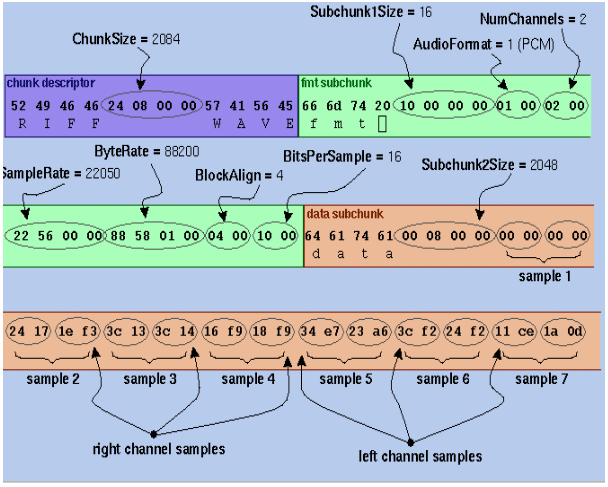


Figure 3: Wave file format

So in this example number of channel are 2. Bits per sample are 16 that indicate16 bits are required for storing sample data for each channel. The value of bits per sample may be 8, 16, 24 or 32.The samples of each channel are consecutively store. If the number of channel is 1 means sound is mono and sample data is continuously store. This scheme is based on audio distribution among different channel as in this case we are implementing for two channel wave file. We divide the process in two parts. First part consists of encryption process or the shares construction and other part is the decryption process or the shares reconstruction. Following is the algorithm for the encryption process and is illustrated in the figure 4.

3.1 Encryption Process

1. Firstly take two channel wave file i.e. stereo file.

2. Using header information finds out the length of the wave file using following formula:

Number of seconds=Number of samples/(number of tracks * sample per second)

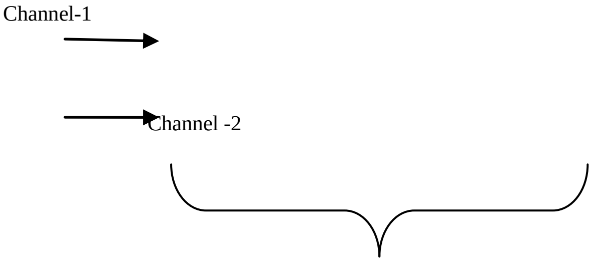
3. Divide the wave file data into ‘n’ parts according to the length of wave file.

4. Create two share files and copy the header information as it is in both the shares.

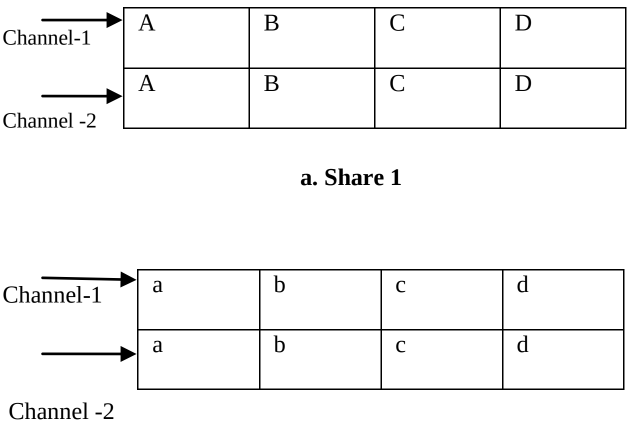
5. Copy the first part of first channel into both channels of first share and first part of second channel into both channel of second share.

6. For the second part both the shares repeat the same process as mentioned in step 5 only interchange the channels.

7. Repeat step 5 and 6 till all parts are copied into shares.



Wave file is divided in 4 parts



Channel-1	A	B	C	D
Channel -2	A	B	C	D

a. Share 1

Channel-1	a	b	c	d
Channel -2	a	b	c	d

b. Share 2

Figure 4: Distribution among two channels

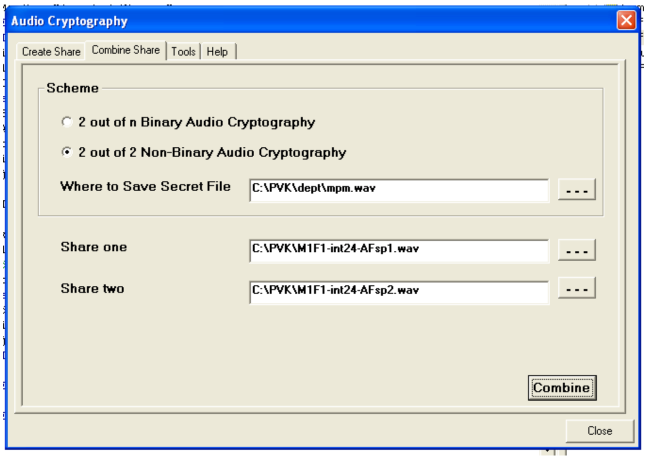
3.2 Decryption Process

After the encryption process has done the share 1 and share 2 are created. But by playing the individual share we will not get the original sound file/wave file. For the original wave file, we need to play both the shares simultaneously.

4. EXPERIMENTAL RESULTS

We have made an application in Visual Basic 6.0 and tested the system for the two channel wave files. In this section, we give some experiments to testify the performance of the proposed algorithm. In experiments, we use the 'M1F1-int12-AFsp.wav' as audio file and by using encryption as discussed in previous section two shares 'M1F1-int24-AFsp1.wav' and 'M1F1-int12-AFsp2.wav' are created. The changes made in the wave file and the original wave file can be identified by the waveforms output. So we have shown that results also. Our method gives very good performance and successfully creates the shares and can combines the shares to get the original wave file.

This scheme is suitable for two channel wave file. Also it will take very less time to create the shares.



Audio Cryptography

Scheme

○ 2 out of n Binary Audio Cryptography

● 2 out of 2 Non-Binary Audio Cryptography

Where to Save Secret File: C:\PVK\dept\mpm.wav

Share one: C:\PVK\M1F1-int24-AFsp1.wav

Share two: C:\PVK\M1F1-int24-AFsp2.wav

Figure 5: Shares creation for Non Binary ACS

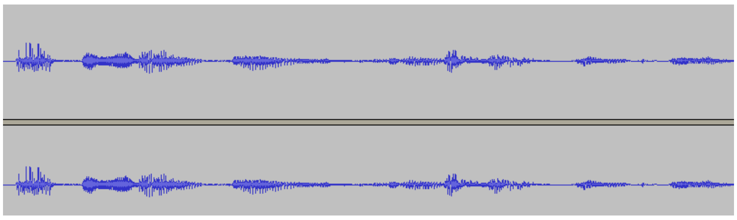


Figure 6: Original file waveform

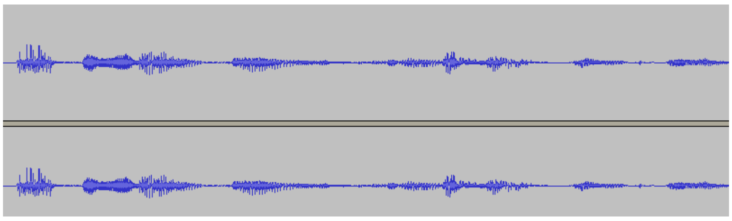


Figure 7: Share1 waveform

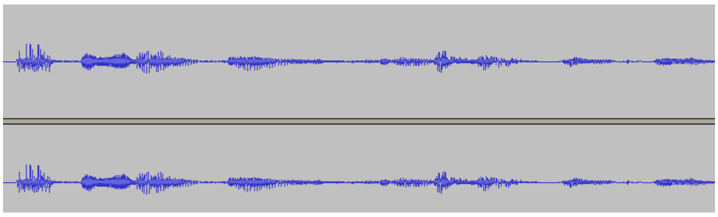


Figure 8: Share 2 waveform

5. CONCLUSIONS

Audio Secret Sharing Scheme is a special type of secret sharing scheme in which the secret is itself an audio file. In this paper we have done the literature survey on the different audio cryptography schemes and also implemented 2-out-2 non binary audio cryptography scheme. This scheme uses the technique of distribution among different channel and we have successfully implemented the scheme for the two channel wave file.

6. REFERENCES

[1] Menezes, A., Oorschot, P. V., Vanstone, S.,"Handbook of Applied Cryptography", CRC Press, 1996

[2] G. Blakley, "Safeguarding Cryptographic Keys", in Proc. American Federation of Information Processing Societies (AFIPS) Arlington, VA, June 1979, vol. 48, pp. 313-317.

[3] Shamir, A.,"How to share a secret", Commun. Of the ACM, 22 (11), pp. 612-613, 1979.

[4] Naor, M., Shamir, A., "Visual cryptography", Eurocrypt 94, Springer-Verlag LNCS Vol. 950, pp. 1-12, 1995.

[5] Y. Desmedt, S. Hou and J. Quisquater, "Audio and optical cryptography," in Advances in Cryptology-Asiacrypt'98, Springer-Verlag LNCS, pp. 392-404.

[6] Ching-Nung Yang, "Improvements on Audio and Optical Cryptography", in Journal of Information Science and Engineering, May 2002, vol. 18, Number 3, pp 381-391

[7] Lin, C. C., Laih, C. S., Yang, C. N., "New Audio Secret Sharing Schemes With Time Division Technique", J. of Information Science and Engineering, 19, pp. 605-614, 2003.

[8] Socek, Daniel dan Spyros S. Magliveras. General Access Structure in Audio Cryptography. in IEEE International Conference on Electro Information Technology (EIT 2005), May 22-25, 2005, Lincoln NE, USA.

[9] Mohammad Ehdaie, Taraneh Eghlidos, Mohammad Reza Aref, "A Novel Secret Sharing Scheme from Audio Perspective "2008 IEEE International al Symposium on Telecommunications 16-19 June pp 13-18

[10] http://ccrma.standford.edu/courses/422/project/waveform